AMENDMENTS TO THE CLAIMS

This listing of claims replaces all prior versions of claims in the application.

Listing of claims:

1-22 (Cancelled).

23. (Currently Amended) A data reproduction apparatus ~~(200)~~ decrypting encrypted content data to reproduce content data, comprising:

a data reproduction unit ~~(1500)~~ to reproduce said encrypted content data, and

a data storage unit ~~(120)~~ storing said encrypted content data and an encrypted content key ~~that is a content key directed to decrypt said encrypted content data in an encrypted form decryptable with a first decryption key unique to said data reproduction unit~~, and providing said encrypted content data and said encrypted content key to said data reproduction unit, wherein said encrypted content key is a content key directed to decrypt said encrypted content data in an encrypted form decryptable with a first decryption key unique to said data reproduction unit;

wherein said data reproduction unit comprises

a session key generation unit ~~(1520)~~ generating a session key updated at every access to obtain said content key with respect to said data storage unit,

a first encryption processing unit ~~(1540)~~ encrypting said session key using a public encryption key that can be decrypted at said data storage unit and that is unique to said data

storage unit, and providing said encrypted session key to said data storage unit,

a first decryption processing unit ~~(1506)~~ using said session key to decrypt said encrypted content key obtained from said data storage unit in an encrypted form with said session key,

a first key hold unit ~~(1540)~~ prestoring said first decryption key,

a second decryption processing unit ~~(1530)~~ extracting said content key by applying a decryption process on an output from said first decryption processing unit using said first decryption key stored in said first key hold unit, and

a third decryption processing unit ~~(1520)~~ receiving said encrypted content data read out from said data storage unit to decrypt said encrypted content data using a content key extracted by said second decryption processing unit to extract content data.

24. (Currently Amended) The data reproduction apparatus according to claim 23, said content data being coded audio data coded according to a coding scheme to reduce an amount of data,

wherein said data reproduction unit comprises

an audio decoding unit ~~(1508)~~ reproducing audio data based on said coding scheme from said coded audio data, and

a digital-analog converter ~~(1512)~~ converting said reproduced audio data into an analog signal.

25. (Previously Presented) The data reproduction apparatus according to claim 23, wherein said data reproduction unit is provided in a security region that cannot be read out by a third party.

26. (Currently Amended) The data reproduction apparatus according to claim 23, wherein said data storage unit ~~(120)~~ comprises

a record unit ~~(1412)~~ to store data applied to said data storage unit,

a second key hold unit ~~(1401)~~ storing said public encryption key unique to said data storage unit, and that can supply said public encryption key to said data reproduction unit,

a third key hold unit ~~(1402)~~ storing a second decryption key used to decrypt data encrypted with said public encryption key,

a fourth decryption processing unit ~~(1404)~~ using said second decryption key to decrypt said first session key transmitted from said data reproduction unit in an encrypted form by said public encryption key, and

a second encryption processing unit ~~(1406)~~ encrypting encrypted content key stored in said recording unit using said first session key extracted at said fourth decryption processing unit for output.

27. (Previously Presented) The data reproduction apparatus according to claim 23, wherein said data storage unit is detachable with respect to said data reproduction unit.

28. (Currently Amended) A data reproduction apparatus ~~(300, 400)~~ decrypting encrypted content data to reproduce content data, comprising:

a data reproduction unit ~~(1500)~~ decrypting said encrypted content data using a content key directed to decrypt said encrypted content data to reproduce content data, and

a data storage unit ~~(130, 140)~~ storing said encrypted content data and said content key, and encrypting a first session key differing for every access to obtain said content key into a form decryptable by a unique decryption key unique to said data reproduction unit for supply to said data reproduction unit,

wherein said data reproduction unit comprises

a first key hold unit ~~(1540)~~ prestoring said unique decryption key,

a first decryption processing unit ~~(1530)~~ applying a decryption processing using said unique decryption key which is an output from said first key hold unit,

a first session key generation unit ~~(1522)~~ generating a second session key updated for every access to obtain said content key with respect to said data storage unit,

a first encryption processing unit ~~(1554)~~ encrypting and applying to said data storage unit said second session key using a first session key that is encrypted in a form decryptable with said unique decryption key supplied from said data storage unit and decrypted at said first decryption processing unit, and

a second decryption processing unit ~~(1556)~~ decrypting for said second session key said content key supplied from said data storage unit in an encrypted form decryptable by said unique decryption key and further encrypted with said second session key,

said first decryption processing unit extracting said content key by applying a further decryption process on the output from said second decryption processing unit using said unique decryption key,

wherein said data reproduction unit further comprises a third decryption processing unit ~~(1520)~~ receiving said encrypted content data supplied from said data storage unit to decrypt said receive encrypted content data using a content key extracted by said first decryption processing unit to extract content data.

29. (Previously Presented) The data reproduction apparatus according to claim 28,

wherein said content data is coded audio data encoded by a coding scheme to reduce an amount of data,

wherein said data reproduction unit further comprises

an audio decoding unit reproducing audio data based on said coding method from said coded audio data, and

a digital-analog converter converting said reproduced audio data into an analog signal.

30. (Previously Presented) The data reproduction apparatus according to claim 29, wherein said data reproduction unit has at least said first key hold unit, said first decryption processing unit, said second decryption processing unit and said third decryption processing unit provided in a security region that cannot be read out by a third party.

31. (Currently Amended) The data reproduction apparatus according to claim 28, wherein said data storage unit ~~(130, 140)~~ comprises

a recording unit ~~(1412)~~ to store data applied to said data storage unit,

a second session key generation unit ~~(1450)~~ generating said first session key,

a second encryption processing unit ~~(1452)~~ applying an encryption process using a public encryption key unique to said data reproduction unit and directed to apply encryption that can be decrypted with said unique decryption key,

a fourth decryption processing unit ~~(1454)~~ using said first session key to decrypt said second session key transmitted from said data reproduction unit in an encrypted form with said first session key, and

a third encryption processing unit ~~(1456)~~ carrying out an encryption process by said first session key extracted at said fourth decryption processing unit for output,

said content key stored in said recording unit being encrypted at said second encryption processing unit and further encrypted at said third encryption processing unit to be supplied to said data reproduction unit.

32. (Previously Presented) The data reproduction apparatus according to claim 28, wherein said data storage unit is a memory card detachable with respect to said data reproduction unit.

33. (Currently Amended) The data reproduction apparatus according to claim 31, further comprising an authentication data hold unit ~~(1560)~~ storing and supplying to said data storage unit

authentication data unique to said data reproduction unit together with said public encryption key in an encrypted form decryptable by an authentication key at said data storage unit,

wherein said data storage unit ~~(140)~~ comprises

a fifth decryption processing unit ~~(1460)~~ decrypting and extracting said authentication data and said public encryption key applied from said data reproduction unit in an encrypted form by said authentication key, and

control means carrying out an authentication process to determine whether to output said content key to a data reproduction unit from which said authentication data is output based on said authentication data extracted by said fifth decryption processing unit.

34. (Currently Amended) A data reproduction apparatus ~~(500, 600)~~ decrypting encrypted content data to reproduce content data, comprising:

a data reproduction unit decrypting said encrypted content data using a content key directed to decrypt said encrypted content data to reproduce content data, and

a data storage unit ~~(150, 160)~~ storing said encrypted content data and said content key, and encrypting and supplying to said data reproduction unit a first session key differing for every access to obtain said encrypted content data in an encrypted form decryptable by a unique decryption key unique to said data reproduction unit,

wherein said data reproduction unit comprises

a key hold unit ~~(1540)~~ prestoring said unique decryption key,

a first decryption processing unit ~~(1530)~~ decrypting for said unique decryption key said first session key encrypted in a form decryptable with said unique decryption key supplied from said data storage unit for extraction,

a session key generation unit ~~(1552)~~ generating a second session key updated for every access to obtain said content key with respect to said data storage unit,

a first encryption processing unit ~~(1554)~~ encrypting and providing to said data storage unit said second session key by said first session key,

a second decryption processing unit ~~(1556)~~ decrypting for said second session key said content data supplied from said data storage unit in an encrypted form with said second session key, and

a third decryption processing unit ~~(1520)~~ receiving said encrypted content data supplied from said data storage unit based on an output of said second decryption processing unit to extract content data.

35. (Currently Amended) The data reproduction apparatus according to claim 34, further comprising an authentication data hold unit ~~(1560)~~ storing, in an encrypted form decryptable by an authentication key, a public encryption key that is an encryption key unique to said data reproduction unit and directed to apply encryption that is decryptable with said unique decryption key and authentication data unique to said data reproduction unit, and that can output the stored public encryption key and authentication data to said data storage unit.

36. (Previously Presented) The data reproduction apparatus according to claim 35, wherein said data storage unit is detachable with respect to said data reproduction apparatus.

37. (Currently Amended) The data reproduction apparatus according to claim 34 wherein said content key is stored in said recording unit in an encrypted form decryptable with a predetermined second decryption key by said data reproduction apparatus,

wherein said data reproduction unit further comprises a fifth decryption processing unit ~~(1572)~~ to carry out decryption using a predetermined second decryption key,

wherein said fifth decryption processing unit receives as a decrypted result for said second session key by said second decryption processing unit said content key supplied from said data storage unit in an encrypted form decryptable with said second decryption key and further encrypted with said second session key, and decrypting said content key for said second decryption key to provide the decrypted content key to said third decryption processing unit.

38. (Previously Presented) The data reproduction apparatus according to claim 34, wherein said data storage unit is detachable with respect to said data reproduction apparatus.

39. (Previously Presented) The data reproduction apparatus according to claim 34, further comprising an interface for connection to a portable telephone network.

40. (Previously Presented) The data reproduction apparatus according to claim 39, further comprising a conversation processing unit to carry out conversation via said interface.

41. (Previously Presented) The data reproduction apparatus according to claim 34, wherein said data storage unit is a memory card detachable with respect to said data reproduction unit.

42. (Previously Presented) The data reproduction apparatus according to claim 34, wherein said data reproduction unit has at least said key hold unit, said first decryption processing unit, said second decryption processing unit and said third decryption processing unit provided in a security region that cannot be read out by a third party.

43. (Currently Amended) The data reproduction apparatus according to claim 34, wherein said data storage unit ~~(150, 160)~~ comprises

a recording unit ~~(1412)~~ to store data applied to said data storage unit,

a second session key generation unit ~~(1450)~~ generating said first session key,

a second encryption processing unit ~~(1452)~~ encrypting said first session key generated at said second session key generation unit by a public encryption key unique to said content data reproduction unit and directed to apply encryption that can be decrypted with said unique decryption key,

a fourth decryption processing unit ~~(154)~~ to decrypt, using said first session key, said second session key transmitted from said data reproduction unit in an encrypted form with said first session key, and

a third encryption processing unit ~~(1456)~~ applying an encryption process by said second session key extracted at said fourth decryption processing unit for output,

wherein said content key stored in said recording unit is encrypted at said third encryption processing unit and supplied to said data reproduction unit.

44. (Currently Amended) The data reproduction apparatus according to claim 35, wherein said data storage unit ~~(150, 160)~~ comprises

a recording unit ~~(1412)~~ to store data applied to said data storage unit,

a fourth decryption processing unit ~~(1460)~~ decrypting using an authentication key said public encryption key and said authentication data that are in an encrypted form decryptable by said authentication key to extract said public encryption key and said authentication data,

a control unit ~~(1420)~~ providing control of an authentication process determining whether said content key is to be output or not to a data reproduction unit from which said authentication data is output based on said authentication data extracted at said fourth decryption processing unit,

a second session key generation unit ~~(1450)~~ generating said first session key,

a second encryption processing unit ~~(1452)~~ encrypting said first session key generated at said second session key generation unit by said public encryption key extracted at said fourth decryption, using said first session key, processing unit,

a fourth decryption processing unit ~~(1454)~~ to decrypt said second session key transmitted from said data reproduction unit in an encrypted form with said first session key, and

a third encryption processing unit ~~(1456)~~ carrying out an encryption process with said second session key extracted at said fourth decryption processing unit for output,

wherein said content key stored in said recording unit is encrypted at said third encryption processing unit to be supplied to said data reproduction unit.

45. (Currently Amended) A data reproduction module ~~(1500)~~ to be loaded in a data reproduction apparatus decrypting encrypted content data to reproduce content data, comprising:

a first key hold unit ~~(1540)~~ prestoring a first decryption key unique to said data reproduction module,

a first decryption processing unit ~~(1530)~~ decrypting for said first decryption key a first session key supplied from a source external to said data reproduction module in an encrypted form that can be decrypted with said first decryption key for every access to obtain a content key which is a decryption key directed to decrypt said encrypted content data, and extracting said decrypted first session key,

a session key generation unit ~~(1552)~~ generating a second session key updated for every access to obtain said content key with respect to a source external to said data reproduction module,

an encryption processing unit ~~(1554)~~ encrypting said second session key using said first session key for output to an external source to said data reproduction module,

a second decryption processing unit ~~(1556)~~ using said second session key to decrypt said content key encrypted with said second session key and supplied from an external source to said data reproduction module, and

a third decryption processing unit ~~(1520)~~ receiving and decrypting said encrypted content data supplied from an external source to said data reproduction module, based on an output of said second decryption processing unit to extract content data.

46. (Currently Amended) The data reproduction module according to claim 45, further comprising an authentication data hold unit ~~(1560)~~ storing a public encryption key unique to said data reproduction module and which is an encryption key that can be decrypted with said first decryption key and authentication data unique to said data reproduction module in an encrypted form that can be decrypted by an authentication key at an external source to said data reproduction module, and that can output the stored public encryption key and authentication data to an external source to said data reproduction module.

47. (Currently Amended) The data reproduction module according to claim 45, wherein said content key is input from an external source to said data reproduction module in an encrypted form with said second session key, and said second decryption processing unit ~~(1556)~~ provides a decrypted result to said third decryption processing unit ~~(1520)~~ as a content key directed to decrypt said encrypted content data.

48. (Currently Amended) The data reproduction module according to claim 45, wherein said content key is input from an external source to said data reproduction module in an encrypted form decryptable with said first decryption key, and further encrypted with said second session key,

wherein said first decryption processing unit decrypts using said first decryption key a content key in an encrypted form decryptable with said first decryption key which is an output of said second decryption processing unit ~~(1556)~~ to extract and provide to said third decryption processing unit ~~(1520)~~ said content key.

49. (Currently Amended) The data reproduction module according to claim 45, wherein said content key is input from an external source to said data reproduction module in an encrypted form that can be decrypted with said second decryption key, and encrypted with said second session key,

wherein said data reproduction module further comprises

a second key hold unit ~~(1570)~~ prestoring said second decryption key, and

a fourth decryption processing unit ~~(1572)~~ using said second decryption key to decrypt said content key subjected to encryption that can be decrypted with said second decryption key output from said second decryption processing unit ~~(1556)~~ to extract and provide to said third decryption processing unit ~~(1520)~~ said content key.

50. (Currently Amended) The data reproduction module according to claim 45, wherein said content data is coded data coded with a coding scheme to reduce an amount of data,

said data reproduction module further comprising a decoding unit ~~(1808)~~ reproducing data based on said coding scheme from said coded data.

51. (Currently Amended) The data reproduction module according to claim 45, wherein said content data is coded audio data coded with a coding scheme to reduce an amount of data,

said data reproduction module further comprising:

an audio decoding unit ~~(1808)~~ reproducing audio data based on said coding scheme from said coded audio data, and

a digital-analog converter ~~(1512)~~ converting said reproduced audio data into analog signals.

52. (Previously Presented) The data reproduction module according to claim 45, wherein said data reproduction module is a tamper resistance module.

53. (Currently Amended) A data reproduction apparatus ~~(300, 400, 500, 600)~~ to be loaded with a data recording apparatus ~~(130, 140, 150, 160)~~ storing encrypted content data and a content key which is a decryption key directed to decrypt said encrypted content data to obtain content data, and encrypting a first session key differing for every access to obtain said encrypted content data into a form decryptable with a unique decryption key unique to said data reproduction apparatus, said data reproduction apparatus reproducing said encrypted content data stored in said data recording apparatus using a content key stored in said data recording apparatus, comprising:

a first interface ~~(1200)~~ to attach said data recording apparatus and carry out data transfer with said data recording apparatus,

a key hold unit ~~(1540)~~ prestoring a unique key unique to said data reproduction apparatus,

a first decryption processing unit ~~(1530)~~ using said unique decryption key to decrypt a first session key updated for every access to obtain said content key and supplied from said data recording apparatus in an encrypted form that can be decrypted with said unique decryption key unique to said data reproduction apparatus,

a session key generation unit ~~(1552)~~ generating a second session key updated for every access to obtain said encrypted content key with respect to said data recording apparatus,

an encryption processing unit ~~(1554)~~ encrypting said second session key using said first session key to supply said encrypted session key to said data recording apparatus,

a second decryption processing unit ~~(1556)~~ using said second session key to decrypt said content key encrypted with said second session key and supplied from said data recording apparatus,

a third decryption processing unit ~~(1520)~~ receiving and decrypting said encrypted content data read out from said data recording apparatus based on an output of said second decryption processing unit to extract content data.

54. (Currently Amended) The data reproduction apparatus according to claim 53, further comprising an authentication data hold unit ~~(1560)~~ storing a public encryption key which is an encryption key unique to said data reproduction apparatus and decryptable with said first decryption key and authentication data unique to said data reproduction apparatus in an encrypted form that can be decrypted by an authentication key at said data recording apparatus, and providing the stored public encryption key and authentication data to said data recording apparatus.

55. (Currently Amended) The data reproduction apparatus according to claim 53, wherein said content key is encrypted with said second session key and supplied from said data recording apparatus ~~(150)~~, and said second decryption processing unit ~~(1556)~~ provides a decrypted result to said third decryption processing unit ~~(1520)~~ as a content key directed to decrypt said encrypted content data.

56. (Currently Amended) The data reproduction apparatus according to claim 53, wherein said content key is encrypted in a form decryptable with said first decryption key, and encrypted with said second session key to be supplied from said data recording apparatus ~~(130, 140)~~,

wherein said first decryption processing unit uses said first decryption key to decrypt an encrypted content key that can be decrypted with said first decryption key which is an output of said second decryption processing unit ~~(1556)~~ to extract and provide to said third decryption processing unit ~~(1520)~~ said content key.

57. (Currently Amended) The data reproduction apparatus according to claim 53, wherein said content key is encrypted in a form decryptable with said second decryption key, and encrypted with said second session key to be supplied from said data recording apparatus ~~(160)~~,

said data reproduction apparatus further comprising:

a second key hold unit ~~(1570)~~ prestoring said second decryption key, and

a fourth decryption processing unit ~~(1572)~~ using said second decryption key to decrypt said content key in an encrypted form decryptable with said second decryption key output from said second decryption processing unit ~~(1556)~~ to extract and provide to said third decryption processing unit ~~(1520)~~ said content key.

58. (Currently Amended) The data reproduction apparatus according to claim 53, wherein said content data is coded data encoded by a coding scheme to reduce an amount of data,

said data reproduction apparatus further comprising a decoding unit ~~(1808)~~ reproducing data based on said coding scheme from said coded data.

59. (Currently Amended) The data reproduction apparatus according to claim 53, wherein said content data is coded audio data coded by a coding scheme to reduce an amount of data,

said data reproduction apparatus comprising:

an audio decoding unit ~~(1808)~~ reproducing audio data based on said coding scheme from said coded audio data, and

a digital-analog converter ~~(1512)~~ converting said reproduced audio data into analog signals.

60. (Previously Presented) The data reproduction apparatus according to claim 53, further comprising a second interface connected to a portable telephone network.

61. (Previously Presented) The data reproduction apparatus according to claim 60, further comprising a conversation processing unit to carry out conversation via said second interface.

62. (Previously Presented) The data reproduction apparatus according to claim 53, said data reproduction apparatus comprising a security region that cannot be read out by a third party,

wherein at least said first key hold unit, said first decryption processing unit, said second decryption processing unit and said third decryption processing unit are provided in said security region.

63. (Previously Presented) The data reproduction apparatus according to claim 53, said data reproduction apparatus including a security region that cannot be read out by a third party,

wherein at least said first key hold unit, said second key hold unit, said first decryption processing unit, said second decryption processing unit, said third decryption processing unit, and said second decryption processing unit are provided in said security region.